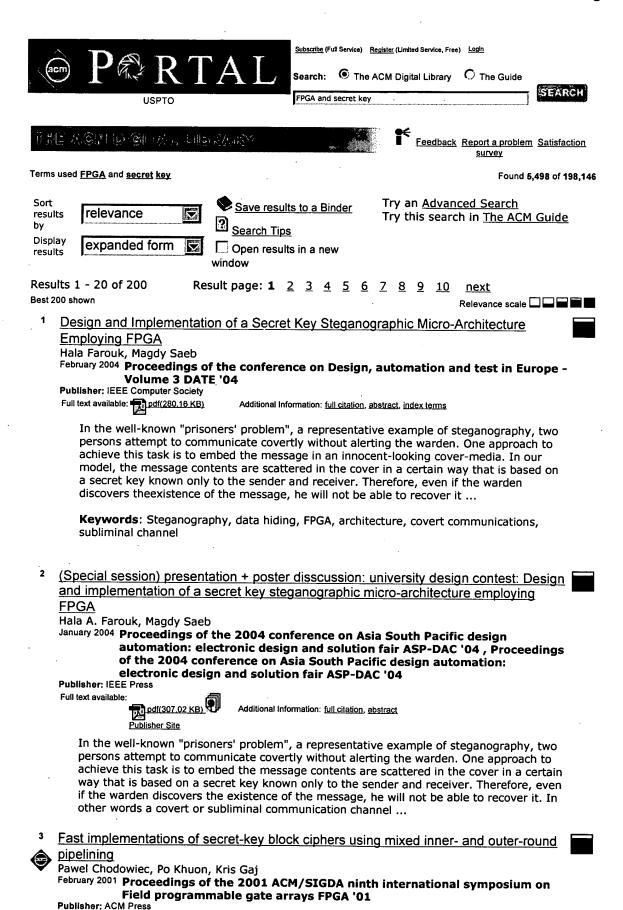
EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S30 5	157	726/8.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 11:59
S30 6	1377	326/39.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:01
S30 7	1154	713/189.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:02
S30 8	682	713/170.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:02
S30 9	606	713/165.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:03
S31 0	1688	713/193.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:03
S31 1	459	713/194.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:03
S31 2	3606	(FPGA) and (hash or MAC)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:05
S31 3	3861	(FPGA) and (hash\$4 or MAC or message adj2 authenticat\$4 adj4 code)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:07

EAST Search History

S31 4	19657	symmetric near3 key or secret near3 key	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:06
S31 5	364	S313 and S314	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:06
S31 6	38858	(FPGA) or (field adj2 program\$5 adj3 gate adj4 array)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:07
S31 7	4269	S316 and (hash\$4 or MAC or message adj2 authenticat\$4 adj4 code)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:07
S31 8	382	S316 and (hash\$4 or MAC or message adj2 authenticat\$4 adj4 code) and S314	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:08
S31 9	1	(FPGA and chip and nonvolatile and (secret or symmetric) and key and MAC and external).CLM.	US-PGPUB; USPAT	OR	ON	2007/02/28 12:09



Additional Information: full citation, abstract, references, citings, index terms

Full text available: pdf(691,29 KB)

The new design methodology for secret-key block ciphers, based on introducing an optimum number of pipeline stages inside of a cipher round is presented and evaluated. This methodology is applied to five well-known modern ciphers, Triple DES, Rijndael, RC6, Serpent, and Twofish, with the goal to first obtain the architecture with the optimum throughput to area ratio, and then the architecture with the highest possible throughput. All ciphers are modeled in VHDL, and implemented using Xilinx ...

Keywords: AES, fast architectures, pipelining, secret-key ciphers

Cellular and Cryptographic Applications: Cryptographic rights management of FPGA intellectual property cores



Tom Kean

February 2002 Proceedings of the 2002 ACM/SIGDA tenth international symposium on Field-programmable gate arrays FPGA '02

Publisher: ACM Press

Full text available: pdf(171.79 KB)

Additional Information: full citation, abstract, references, index terms

As the capacity of FPGA's increases to millions of equivalent gates the use of Intellectual Property (IP) cores becomes increasingly important to control design complexity. FPGA's are becoming platforms for integrating a system solution from components supplied by independent vendors in the same way as printed circuit boards provided a platform for earlier generations of designers. However, the current commercial model for IP cores involves large up-front license fees reminiscent of ASIC NRE cha ...

Keywords: FPGA, cryptography, intellectual property, rights management

Security on FPGAs: State-of-the-art implementations and attacks



August 2004 ACM Transactions on Embedded Computing Systems (TECS), Volume 3 Issue 3

Publisher: ACM Press

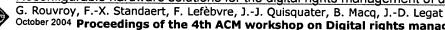
Full text available: pdf(296,79 KB)

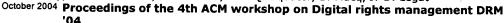
Additional Information: full citation, abstract, references, index terms

In the last decade, it has become apparent that embedded systems are integral parts of our every day lives. The wireless nature of many embedded applications as well as their omnipresence has made the need for security and privacy preserving mechanisms particularly important. Thus, as field programmable gate arrays (FPGAs) become integral parts of embedded systems, it is imperative to consider their security as a whole. This contribution provides a state-of-the-art description of security issues ...

Keywords: Cryptography, FPGA, attacks, cryptographic applications, reconfigurable hardware, reverse engineering, security

Reconfigurable hardware solutions for the digital rights management of digital cinema





Publisher: ACM Press

Full text available: pdf(440.86 KB)

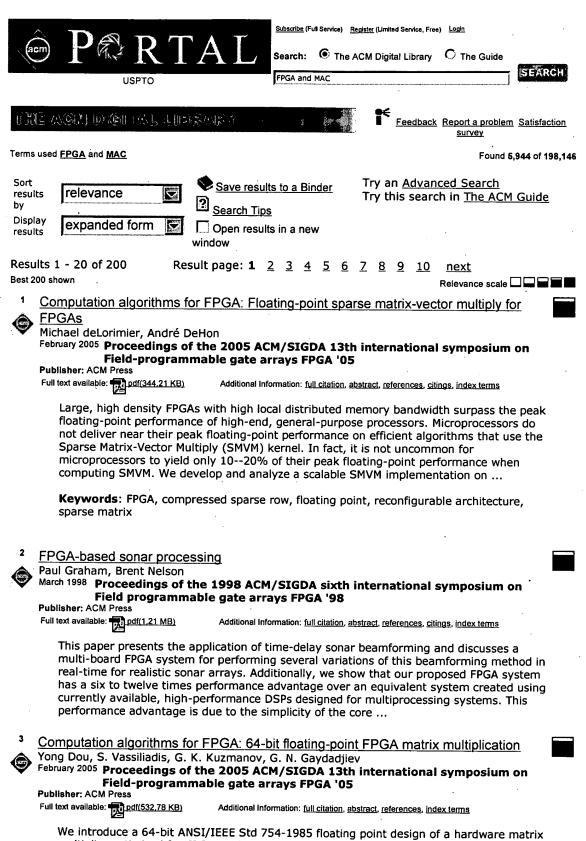
Additional Information: full citation, abstract, references, index terms

This paper presents a hardware implementation of a decoder for Digital Cinema images. This decoder enables us to deal with image size of 2K with 24 frames per second and 36 bits per pixels. It is the first implementation known nowadays that perfectly fits in one single Virtex-II® FPGA and includes AES decryption, JPEG 2000 decompression and fingerprinting blocks. This hardware offers therefore high-quality image processing as well as robust security.

Keywords: AES, DRM, FPGA, JPEG 2000, digital cinema, watermarking

An Improved FPGA Implementation of the Modified Hybrid Hiding Encryption Algorithm (MHHEA) for Data Communication Security Hala A. Farouk, Magdy Saeb





multiplier optimized for FPGA implementations. A general block matrix multiplication algorithm, applicable for an arbitrary matrix size is proposed. The algorithm potentially enables optimum performance by exploiting the data locality and reusability incurred by the general matrix multiplication scheme and considering the limitations of the I/O bandwidth and the local storage volume. We implement a scalable I ...

Keywords: FPGA, floating-point, matrix multiplication

Novel FPGA applications: CUSP: a modular framework for high speed network applications on FPGAs



Graham Schelle, Dirk Grunwald

February 2005 Proceedings of the 2005 ACM/SIGDA 13th international symposium on Field-programmable gate arrays FPGA '05

Publisher: ACM Press

Full text available: pdf(547.03 KB)

Additional Information: full citation, abstract, references, citings, index terms

For several years now, modern FPGAs have included onchip network related hard cores. These cores include Xilinx's RocketIO and Altera's RapidIO serial transceivers. However, to use these cores in a complete networking application may be a daunting task to a nonnetworking expert. In addition to the complicated use of these components, the high performance needs of modern networking applications require designs that are optimized for low latency and a moderately high clock rate. Therefore to meet ...

Keywords: networking, parallelism, reconfigurable hardware, speculation

Security: The shunt: an FPGA-based accelerator for network intrusion prevention

Nicholas Weaver, Vern Paxson, Jose M. Gonzalez

February 2007 Proceedings of the 2007 ACM/SIGDA 15th international symposium on Field programmable gate arrays FPGA '07

Publisher: ACM Press

Full text available: pdf(240.27 KB)

Additional Information: full citation, abstract, references, index terms

The sophistication and complexity of analysis performed by today's network intrusion prevention systems (IPSs) benefits greatly from implementation using general-purpose CPUs. Yet the performance of such CPUs increasingly lags behind that necessary to process today's high-rate traffic streams. A key observation, however, is that much of the traffic comprising a high-volume stream can, after some initial analysis, be qualified as "likely uninteresting." To this end, we have developed an in-line, ...

Keywords: FPGA, NIC, hardware acceleration, intrusion detection

Parameterized MAC unit implementation

Ming-Chih Chen, Ing-Jer Huang, Chung-Ho Chen

January 2001 Proceedings of the 2001 conference on Asia South Pacific design automation ASP-DAC '01

Publisher: ACM Press

Full text available: pdf(79,23 KB)

Additional Information: full citation, abstract, references, index terms

Ethernet communication devices, such as adapter, hub, bridge and switch, all follow IEEE 802.3 standard protocol. We have designed and implemented an integrated 10/100 Mbps Ethernet MAC (Medium Access Control) mechanism. The MAC unit is used to handle receive/transmit processes of network packet stream. To meet the requirement of different communication devices, we design an automatic MAC unit generator. Users can select the desired number of MAC units through parametric environment setup. \dots

Effective Co-Verification of IEEE 802.11a MAC/PHY Combining Emulation and Simulation Technology

IL-Gu Lee, Seung-Beom Lee, Sin-Chong Park

April 2005 Proceedings of the 38th annual Symposium on Simulation ANSS '05

Publisher: IEEE Computer Society

Full text available: pdf(358.72 KB)

Additional Information: full citation, abstract, index terms

This work presents a system architecture and effective co-verification methodologies for the IEEE 802.11a Medium Access Control (MAC) layer/Physical (PHY) layer implementation. The architecture modeling includes hardware/software partitioning of a total system based on timing measurements from the C/C++ and Verilog design, and analysis of real-time requirements specified in the standard. The system is built on an evaluation platform that contains a Xilinx Virtex-II FPGA and an Altera Excalibur A ...

Design Space Exploration for a Wireless Protocol on a Reconfigurable Platform

[File 2] INSPEC 1898-2007/Feb W3

(c) 2007 Institution of Electrical Engineers. All rights reserved.

[File 6] NTIS 1964-2007/Feb W4

(c) 2007 NTIS, Intl Cpyrght All Rights Res. All rights reserved.

[File 8] Ei Compendex(R) 1884-2007/Feb W3

(c) 2007 Elsevier Eng. Info. Inc. All rights reserved.

[File 34] SciSearch(R) Cited Ref Sci 1990-2007/Feb W3

(c) 2007 The Thomson Corp. All rights reserved.

[File 434] SciSearch(R) Cited Ref Sci 1974-1989/Dec

(c) 2006 The Thomson Corp. All rights reserved.

[File 35] Dissertation Abs Online 1861-2007/Feb

(c) 2007 ProQuest Info&Learning. All rights reserved.

[File 62] **SPIN(R)** 1975-2007/Feb W2

(c) 2007 American Institute of Physics. All rights reserved.

[File 65] Inside Conferences 1993-2007/Feb 28

(c) 2007 BLDSC all rts. reserv. All rights reserved.

[File 99] Wilson Appl. Sci & Tech Abs 1983-2007/Feb

(c) 2007 The HW Wilson Co. All rights reserved.

[File 144] Pascal 1973-2007/Feb W3

(c) 2007 INIST/CNRS. All rights reserved.

[File 266] **FEDRIP** 2007/Jan

Comp & dist by NTIS, Intl Copyright All Rights Res. All rights reserved.

[File 275] Gale Group Computer DB(TM) 1983-2007/Feb 27

(c) 2007 The Gale Group. All rights reserved.

[File 621] Gale Group New Prod.Annou.(R) 1985-2007/Feb 19

(c) 2007 The Gale Group. All rights reserved.

[File 674] Computer News Fulltext 1989-2006/Sep W1.

(c) 2006 IDG Communications. All rights reserved.

*File 674: File 674 is closed (no longer updates).

? s FPGA or field (2n) program? (2n) gate (2n) array? Processing 38937 FPGA 4737778 FIELD

```
4581316
                PROGRAM?
       328464
                GATE
       970443
                ARRAY?
        34329
                FIELD (2N) PROGRAM? (2N) GATE (2N) ARRAY?
S1
        47741
                S FPGA OR FIELD (2N) PROGRAM? (2N) GATE (2N) ARRAY?
  s secret (2n) key? or symmetric (2n) key?
        55484
                SECRET
      1948952
                KEY?
         5774
                SECRET (2N) KEY?
       324275
                SYMMETRIC
      1948952
                KEY?
         1392
                SYMMETRIC (2N) KEY?
S2
         7001
                S SECRET (2N) KEY? OR SYMMETRIC (2N) KEY?
? s MAC or message (2n) authenticat? (2n) code?
       146779
                MAC
       278410
                MESSAGE
        90221
                AUTHENTICAT?
      1322898
                CODE?
          830
                MESSAGE (2N) AUTHENTICAT? (2N) CODE?
                S MAC OR MESSAGE (2N) AUTHENTICAT? (2N) CODE?
S3
       147195
? s s1 and s2 and s3
        47741
                S1
         7001
                S2
       147195
                S3
S4
                S S1 AND S2 AND S3
```